

⑨ 日本国特許庁 (JP)

⑩ 特許出願公開

⑫ 公開特許公報 (A)

昭56-123066

⑮ Int. Cl.³
G 06 F 15/30
15/00

識別記号
1 0 2

庁内整理番号
7737-5B
6974-5B

⑬ 公開 昭和56年(1981) 9 月26日

発明の数 1
審査請求 有

(全 12 頁)

⑭ 取引実行システムのための個人認証方法

⑯ 特 願 昭56-3986

⑰ 出 願 昭56(1981) 1 月16日

優先権主張 ⑱ 1980年 2 月11日 ⑲ 米国(US)
⑳ 120222

㉑ 発 明 者 ドナルド・ジョセフ・チエサレ
ク
アメリカ合衆国カリフォルニア

州ロス・ガトス・ベルブロッサム・ウェイ280番地
⑳ 出 願 人 インターナショナル・ビジネス
・マシーンズ・コーポレーション
アメリカ合衆国10504 ニューヨーク州アーモンク(番地なし)
㉒ 代 理 人 弁理士 頓宮孝一 外 1 名

BEST AVAILABLE COPY

明 細 書

1. 発明の名称 取引実行システムのための個人認証方法

2. 特許請求の範囲

ホスト・プロセッサに接続された端末装置を操作してカードから読取られたカード・データと鍵盤から入力された認証データとの関係を検査する取引実行システムのための個人認証方法にして、前記カード・データ及び可変数を含む取引要求メッセージを前記ホスト・プロセッサへ送信する段階と、

前記ホスト・プロセッサにおいてファイルの認証データ検査欄を前記カード・データによってアクセスする段階と、

前記アクセスされた認証データ検査欄と前記可変数とを結合し、その結果を暗号化する段階と、

前記暗号化の結果を含む取引応答メッセージを前記端末装置へ返送する段階と、

前記端末装置において前記取引応答メッセージ

における前記暗号化の結果を復号し、前記復号された認証データ検査欄と前記鍵盤から入力された認証データとを比較する段階と、

より成る取引実行システムのための個人認証方法。

3. 発明の詳細な説明

この発明は取引実行システムに関するものであり、特に、ホスト計算機が中央にデータ・ベースをもち、遠隔端末装置との通信によつて取引を実行するシステムを操作する方法に関する。例えば、これは特定の、ないし提携金融機関によつて発行された機械可読な暗証カードを入力すると同時に個人暗証番号を入力することに対応して、現金の払出しや金融機関同志の振替等を行うシステムであつて、この場合個人暗証番号は、暗証カード上のデータから得られるようになっていてもよいし、そうでなくてもよいものとする。

口座その他の情報を記憶した中央データベースをもつホスト計算機と端末装置が交信して現金の払出し等の取引を行う取引実行システムの存在は

(1)

—353—

(2)

広く知られている。このようなシステムの例としては、米国特許第3956615号、第3970992号、第3937925号、第4186871号さらに1979年2月2日出願の米国特許未決出願第009384号がある。

端末装置を通じて現金の払出しや預金を行なうこのようなシステムは現代の熾烈なビジネス環境のもとで、銀行のサービス拡張のために広く用いられている。

この種の端末装置は通常、クレジット・カード上の情報を読み取る機構、鍵盤、表示機構、通帳出し入れ口を具えている。この端末装置は、データ・ベースと連係して操作することも、独立して用いることもできる。

銀行員を介さずに行われる現金の払出しや、その他の銀行取引における安全確保の向上は、各クレジット・カードに個人暗証番号(ID Number)を与えることによつて保証される。クレジット・カードから読み取られた口座番号に対応する暗証番号が鍵盤から入力されたとき、はじめてクレジ

(3)

ット・カード)によつて、独立した(ホストと切り離された状態になつている)端末装置においても、暗証番号を検査することができる。

提携した複数の銀行が発行するクレジット・カードが同一の端末装置で使用される場合には、これらの銀行は、口座番号から暗証番号を作り出す際に、いずれも同一のコードないし算法を用いるか、これらの算法を区別する方策を提供しなければならぬ。

このようなシステムの一つとして暗証番号と口座番号との関係を決めるために、キー番号による算法を用いたものがある。このシステムにおいては、暗証番号と比較するための検査番号を生成するために、線形および非線形演算によつて、口座番号とキー番号が組み合わせられる。前記米国特許第3956615号はこのようなシステムである。

しかしながら複数の銀行が発行したカードを同一端末において用いられる場合には、すべての銀行は同一のキー番号を使わなくてはならず、また口座番号は、すべてのカード上で同一位置になくて

(5)

ット・カードによる取引が可能になる。

このような手続きを決めておけば、盗難ないし拾得カードによる端末装置からの現金引出し等を防止することができる。端末装置がデータ・ベースと連係して用いられる場合には、口座番号と暗証番号との対応性は自由に選ぶことができる。

しかし一方、暗証番号は、所定のコードに従つて口座番号から作り出すこともできる。

前者の場合については後に詳述する。

後者の場合は暗証番号を預金者が自由に選ぶことができるようにするため、カード上には口座番号と一緒に差引値(offset value)を記録しておく。すなわちこの暗証番号は、所定のコードに従つて口座番号から作り出された番号とこの差引値が加え合わされるか或いは組み合わせられた結果得られる番号が自由に選ばれた暗証番号に等しくなるように選ばれている。

このように暗証番号と、カード上の口座番号(および差引値)の間の関係を前もつて決めておけば、暗証番号と口座番号とを関係づける算法(ア

(4)

はならない。

この米国特許のシステムに対する一改良法は、各端末装置に、暗号化されたキーのテーブル(一覧表)を設けることである。このテーブルには、複数提携銀行が用いるキーによる算法、カード上の口座番号の位置(データ・トラック)を示すデータ、差引値その他、鍵盤から入力された暗証番号と比較される検査番号を生成するためのデータが記録される。

このシステムの改良型としては前述の米国特許第4186871号がある。これによればホスト計算機に「仮想金融機関テーブル(VFIT)」を設けている。利用者がクレジット・カードと暗証番号を入力すると、クレジット・カードにおいて指定された銀行に対応する項目を見付け出すために端末装置内の金融機関テーブル(FIT)がまず探索される。もし目的の項目が見付かれれば項目中のデータが用いられてクレジット・カード上の個人データが暗号化され、利用者が入力した暗証番号を検査するために用いられる。

(6)

もし端末装置のF I T中に目的の項目が見付からない場合はホスト計算機のV F I Tの探索が行なわれる。ホストのV F I T中に目的の項目が見付かるとそのデータは端末装置に送り返され、そこで暗証番号の検査が行なわれる。

別の方法としてはクレジット・カード上のデータと暗証番号をホストへ送つて、口座番号と暗証番号の検査(これをP I N検査という)を含む取引の認可をホストで行なうよう指示する制御ビットを、端末装置のF I T中に入れておくこともできる。

端末装置におけるP I N検査に加えてホストで行われるP I N検査については米国特許第3956615号に述べられている。このようなホストのP I N検査においては、端末装置から入力された暗証番号が2重に暗号化されて、カード上のデータと共にホストへ送られる。ホストにおいては、2重に暗号化された暗証番号は1重に復号され、暗号化されている暗証番号のデータ・ベースがカード・データによつてアクセスされる。データ・

(7)

末装置から銀行間で口座への振替を行なつたりすることに不当に利用される弱点も残している。

重大な問題の一つに、端末装置が独立して働く場合にもオンラインで働く場合にも、端末装置における暗号化の算法に関する安全保護の問題がある。

現金支払用端末装置を連日稼動させるには多数の操作員や保守要員が必要になる。たとえば銀行の各支店には現金支払用端末装置の内部に接触できる行員が存在する。この人たちは通常の保守作業のために暗号キーに接することも間々あるでしょう。あるいは多少の訓練を受ければこの人たちが通信回線を盗聴したり、内部回路の電気的信号を測定したりすることにより、不当にキーを知りうることも考えられる。

いちど暗号化のキーを手し、算法が判つてしまえば、膨大な数の口座番号と暗証番号の関連性を生成できることになる。さらにカードの様式、カード上の検証データや差引値の位置を知ることにより、カード・データと自由に選んだ暗証番号

(9)

ベースから取り出された暗号化されている暗証番号は、端末装置から受取つた「2重に暗号化されたものを1重に復号した」暗証番号と比較されてP I N検査が行なわれる。しかしながらこのシステムでは、もしホストにおけるP I N検査が通らなければ取引は認可(承認)されない。すなわちP I N検査は最初からやり直さなければならないことになる。

カード上のデータと鍵盤から入力された暗証番号の算法的關係に基づいたP I N検査が端末装置で行なわれる場合には番号が一致しないともういちど正しい番号を入力しなおすことになり、何回かやり直してもやはりうまく行かなければ取引が拒否される。

クレジット・カードと暗証番号に対し、テーブルとキーを使用する上述の検証方式によつて現金支払用端末装置の安全性は向上し、また多数銀行間が提携して仙行カードによる現金の払出し等ができるようになった。しかしこのシステムでは端末装置内に存在する大額の現金を手したり、弊

(8)

との関連性を確認することもできる。

このことから提携関係にある銀行のいくつかは、カード・データと暗証番号とを関連づける暗号化キーを他行では知り得ないように、P I N検査をそれぞれ自行のホストで行なうべきであると主張している。

しかし前述のとおり、この方法によれば、ホストにおけるP I N検査が通らないと取引を拒否しなければならない。利用者は最初の取引がP I N検査に合格せず拒否されたという表示があつたときには直ちに取引をやり直すことができる。しかしながらこの方法は利用者にとつてもシステムにとつても時間の浪費となり、経費の増大とシステム全体の可用性を低下させることになる。

発明の要約

この発明にかかわる取引実行システムは、検証(validation)番号を含む情報を記憶したデータ・ベースを含むホスト計算機を包含する。この検証番号は口座番号その他のデータを暗号化し

(10)

たものから作り出したものであつても、そうでなくてもよい。ホスト計算機には一つ以上の端末装置が連結され、各端末装置からは口座番号と暗証番号を入力する手段をもつものとする。

この発明においては、端末装置から入力された暗証番号は、第1の暗号キーを用いて暗号化され第1の結果を得る。第1の結果は端末装置で生成された変数と連結され、連結された番号は、さらに第2の暗号キーにより暗号化される。このようにして2重に暗号化された暗証番号が生成される。つぎに2重に暗号化された暗証番号は口座番号その他のデータと共にホストへ送られ、そこで2重に暗号化された番号は第2の暗号キーにより復号され第1の結果に戻される。そして第1の結果はホストのデータ・ベースにある、口座番号に付随する暗証番号と比較される。

ホストにおいて暗証番号と第1の結果とが不一致になつたが、取引自体は承認された、という場合には、ホストは暗証番号と変数を連結して、これを第2の暗号キーによつて暗号化し、暗号化し

(11)

取引認可システムの改善に關する。

当業者には明らかであるが、CPU10は、たとえばIBMシステム/370であつて、データ・ベースに対しVSAN、ISAMおよび/またはSAMを通してアクセスし、DOS/VS、OS/VS1、OS/VS2の元で動くVTAM適用業務を実行するものと仮定してもよい。データ・ベース12は、適用業務を処理するために必要なライブラリーおよび口座に関するファイルを持つている。後者には預金残高、入金・支払の記録等、口座に関する情報および後に詳述する暗証番号が記憶されている。

また2つ以上の金融機関が提携し、相互のデータ処理システムを結合している場合も考えられる。これはCPU10および16を結ぶ図14で示されている。

CPU16は、客先の口座データ等を記憶するデータ・ベース18に接続されている。

B銀行のCPU10は通信ループ36を通して複数の銀行端末装置20、22が接続されている。

(13)

た暗証番号を生成して、条件付きメッセージ中に入れ端末装置へ送り返す。

端末装置は条件付き取引承認メッセージ中の、暗号化された暗証番号を復号して、比較のための暗証番号を生成する。比較の相手は、再入力された第1のキーによつて暗号化された暗証番号である。この代替案としては生成された暗証番号を第1のキーにより復号し、再入力された暗号化されない、ナマの暗証番号と比較する方法もある。

再入力された暗証番号と、条件付き取引承認メッセージ内のデータとの比較の結果、端末装置において取引が承認されることもあり得る。

発明の開示

この発明の内容、目的、利点を、より良く理解するために、参考として図、適用業務を付した説明およびこの発明における種々の新しい特長を以下に示す。

第1図に示すようにこの発明はホストCPU10およびデータ・ベース12を持つ銀行における

(12)

これはSDLC網(ここには図示されていないが)を通して直接に接続されていてもよいし、たとえばIBM3610金融機関通信制御装置24を通して接続されていてもよい。線26は、たとえばCPU10のVTAMによつて制御される通信回線およびNCP/3(回線網制御プログラム第3版)によつて制御されるIBM3704/3705通信制御装置を含むことを示す。制御装置24はデータ・ベース12に含まれるデータの一部である口座データを記憶するために、ディスクットを装備している場合もある。

B銀行のCPU10には端末装置20、22が接続されていることが示されているが、同様にA銀行のCPU16も所要の数の銀行用端末を備えているのが普通である。このような場合には提携銀行は、利用者がどこの銀行の端末から取引を行なつてもよいことを認めている。

この場合、A銀行の発行した機械可読な認証カードの所有者がA銀行の端末装置20に付属するキュッシュ・デイスペンサー28を通じて自分の

(14)

口座から現金を引出したり、あるいは預金、振替、残高等の問合せ、払込み等、何らかの取引を行いたいと考えたとする。

利用者が端末装置 20 を使用して取引を行なうことができるようにするためには、通常まず機械可読な口座カード（認証カードないしクレジット・カード）を機械に挿入し、鍵盤から個人認証番号（PIN）を入力する。口座カードから読み取られたデータには PIN の正当性を検査するための、口座番号の全部または一部が含まれている。この正当性検査すなわち PIN 検査はつぎのようにして行なわれる。

まず、カード・データか PIN のいずれか一方を暗号化し他方と比較する。すなわち暗号化されたカード・データを PIN と比較するか、暗号化された PIN をカード・データと比較するか、である。この暗号化はキー番号の制御の元で行なわれるが、これについては米国特許第 3956615 号および同第 4186871 号に詳述されている。後者には金融機関テーブル（FIT）の存在

(15)

検査に必要なこの情報（これには口座認証の情報も含まれる）はカード読取装置 30 で読み取られるか、鍵盤 32 から入力されるかして、PIN 検査のためホストすなわちこの場合は CPU 16 へ送られる。これについては後に詳述する。これは B 銀行についても同様であつて、口座カード上に記録されたデータから生成されない PIN を B 銀行が発行した場合、端末装置 20、22 に対し B 銀行の利用者から受取つたデータを制御装置 24 または CPU 10 へ、ホスト PIN 検査のために送るよう要求することもありうる。

第 2 図を参照すると、この例では代表的な取引を行なうための端末装置 20 とホスト（制御装置 24 もしくは CPU 10）間の通信が、要求メッセージ 40、取引応答メッセージ 42、状況メッセージ 44 を含む 3 メッセージ・プロトコルに従つて行なわれる。（これは米国特許第 4186871 号に第 5 図と関連しておよび米国特許未決出願第 9384 号に第 12 図と関連して VFIT および取引を処理する対話式の関連メッセージにつ

(17)

特開昭 56-123066(5)

が述べられている。これによれば、A 銀行から発行されたカードを、端末装置 20 で検査するために、端末装置 20 の記憶機構内に A 銀行の暗号キーを記憶できるように考案している。しかしながら A 銀行は B 銀行との提携には同意したものの、CPU 10、制御装置 24、および／または端末装置 20、22 に記憶される A 銀行の FIT 中に暗号キーを入れたくないという状況もありうる。さらに A 銀行は、口座カード上のコード化されたデータから生成されない PIN を利用者へ発行することもありうる。いずれの場合も端末装置 20 は読取装置 30 によつて読み取られた口座カードと、鍵盤 32 から入力された PIN との一致性を検査することはできない。

この状況においては、利用者は表示装置 34 等を通して、取引に必要なもつと詳しい情報を入力するよう要請されることになる。この点については米国特許第 3956615 号および第 4186871 号さらに同未決出願第 009384 号に詳述されている。ホストにおいて行なわれる PIN

(16)

いて詳述されている。)第 3 図を参照すると、この例では B 銀行の端末装置 20 からの通信が、同じメッセージ・プロトコルに従つて B 銀行から A 銀行のホスト 16 へ送られる例が示されている。この場合にも上述の VFIT と対話メッセージが含まれうる。適用業務プログラムによつては、通信時間の短縮、記憶装置の節約、端末装置の利用度向上の目的で、取引の処理が、ホストを構成する 24、10、16 等の装置において分散して行なわれることもある。

第 4 図を参照して、ここではホストにおいて安全かつ最適の初期 PIN 検査を実施するために端末装置 20 が取引要求メッセージ 40 を生成する操作について記述する。

これは PIN が ID カード上のデータから生成されない場合、あるいは PIN とカード・データとの対応を検査するための暗号キーが端末装置に入っていない場合、さらには端末装置で行なわれた PIN 検査が合格せず、ホストに送られてさらに検査が行われる場合等に必要になる。

(18)

上述のいずれかの状況下で、ホストにおける初期PIN検査に不合格となつた場合には、引続き端末装置において再度入力されたPINに基づき検査が行なわれる。これによつてPIN検査のため再度ホストとの通信をやり直さずに済み、口座カードに対応する正しいPINの盗聴による漏洩を防ぐことができる。

端末装置20はプログラム式のマイクロ・プロセッサを備えており、マイクロプログラムの制御の元で働く。これに関しては米国特許第3956615号および同第4186871号に詳述されている。

IDカード38はカード読取装置30によつて読み取られ、金融機関認証データを発生する。このデータは金融機関テーブル(FIT)46をアクセスするのに使用される。FIT46中のデータはAキーの制御の元で復号され、PINキー50を生成する。このキーは金融機関ごとに個別に(一意に)決められているものである。

復号の段階48およびその他すべての暗号化／

(19)

計算機種の番号など、何らかの取引や、端末装置に関連して算法的に一つの番号を生成する。Cキーは通信キーであつて、端末装置とホスト・システム間の通信リンクにおけるデータの安全保障に使用される。

暗号化段階64の出力は64ビットの、2重に暗号化された番号であり、暗号化されたPIN+PAD58の残りの8ビットと連結されて、72ビットの暗号化された認証番号66を形成する。これは取引要求メッセージ40のうちの暗号化された部分である。暗号化されない情報70には、たとえばホストが取引要求を処理するさいに必要なデータ、すなわちカード38から読み取られたデータあるいは鍵盤32から入力された取引の種類、金額(ただしPINは含まれない)等がある。ヘッダー72にはメッセージの種類および端末装置のアドレスが含まれている。第5図を参照して、ホストであるA銀行およびB銀行においてPIN検査が行なわれ、取引応答メッセージ42が生成される過程を以下に示す。

(21)

復号の過程は合衆国政府標準局の発行による「計算機データ保護のための暗号算法」連邦登録Vol. 40、第52、1975年3月17日(月)12134~12138ページに示されたもの(以下これをDES(Data Encryption Standard)と略す)による。当業者には明らかであるが、DESはハードウェアの一部によつて構成されていてもよいし、マイクロコードであつてもよい。

FIT46からは当該金融機関のためのPAD数字52が得られる。これは利用者が鍵盤32から入力したPIN54の数字と連結されて64ビットの番号を生成し、PINキー50の制御の元で段階56においてDESにより暗号化される。暗号化されたPIN+PAD58は64ビットから成り、そのうち56ビットは変数生成機構60によつて生成された変数からの8ビットと連結される。このようにして連結された番号62は、通信キーすなわちCキーの制御の元でDESにより暗号化される。

変数生成機構は、たとえば取引一連番号や紙幣

(20)

B銀行を例にとると、取引要求メッセージ40には、その暗号化されない情報部分70にデータ・ベースをアクセスするための番号が含まれている。この番号はIDカード38から読みとられた利用者口座番号に関連する。

段階74において、データ・ベースをアクセスするための番号が要求メッセージ40から読み取られアドレスまたは探索引き数として認証データを取り出すのに用いられる。認証データはPADと連結されて暗号化された利用者PINであつて、暗号化されたPIN+PADとしてデータ・ベース12に記憶されている。

このように利用者PINはホスト・データ・ベース中に、判然とした形(ナマの形)で記憶されているわけではないので、承認された要員以外の人を読んでも判らないようになつている。

段階76においては第6図に関連して後に詳述するが、取引要求メッセージ上の暗号化されたデータ68が復号される。

段階78においては取引承認の処理で始まり、

(22)

ホスト銀行の適用業務プログラムによつて定められている、口座残高、入金・支払の記録、陸難・紛失カードの検査などが行なわれる。

上述の検査により取引が承認されなければ、段階80においてホスト10は取引応答メッセージ42を作り、段階82において、端末装置20に対し通信による取引を拒否する。

取引が承認された場合には段階78の口座検査に基づき、段階84において、少くとも取引応答メッセージ42の基本部分が作られる。これは前述の米国特許中に詳述されている。

段階86においてはホストPIN検査が行なわれる。この検査は、第4図の段階74においてデータ・ベース12から得られる、暗号化されたPIN+PAD欄と、第5図の段階76において取引要求メッセージから得られるPIN+PADの欄とが比較されて行なわれる。

もしホストPIN検査が合格すれば、段階84において取引応答メッセージ42が生成され、段階82において取引の承認が端末装置20へ送ら

れる。もしホストPIN検査が不合格になれば、段階88において、条件付き承認を示す取引応答メッセージが生成され段階82において端末装置20へ送られる。

段階80または84において生成された、承認または拒否を示す取引応答メッセージの様式は第8図のとおりである。

段階84および88において生成された取引応答メッセージを第11図に示す。このメッセージは条件付き取引承認であることを示し、同時に端末装置内において条件付き取引承認の状況を確認する。

段階88においては応答メッセージ42の中の、PIN検査を要請するビットによつて、暗号化された暗証データ欄90が生成される。これは第7図と関連して後述する。

条件付き承認応答メッセージにおいて、端末装置側では再度ホストとの連結を確立し直すことなく、利用者が正しいPINを再入力することができるようになる。

(23)

第6図を参照する。以下は取引要求メッセージ40の暗号化された欄68から暗号化されたPIN+PADをホストが生成する過程である。段階92においては、暗号化された欄68が、通信キーCを用いて復号される。結果としての64ビットには、変数生成機構60(第4図)からのデータを表わす8ビットの部分が含まれ、また欄68のうち残りの8ビットと連結される56ビットが含まれる。これは暗号化されたPIN+PAD94となり、第4図におけるデータ58に等しく、段階86においてホストPIN検査に用いられる(第5図)。

第7図を参照する。段階88(第5図)において、条件付き承認を示す取引応答メッセージ42のために、暗号化されたデータ・ベース中の認証番号90を、ホストCPU10が生成する過程を以下に示す。この方法によればPIN認証データの要素(この例ではデータ・ベース中のPIN+PAD)は、通信回線に乘らない。したがって盗聴されることはないから、端末装置20を操作し

(25)

(24)

て現金を不正に払出されるおそれもない。

変数生成機構においては以下のいずれを行つてもよい。第1の方法では、変数は変数生成機構により単純に生成されたものであつてもよい。これは段階92において復号の出力として用いられる(第6図)。第2の方法は乱数を用いるものである。第3の方法としては、たとえば取引要求メッセージ中のある量(たとえば取引一連番号など)から算法的に生成してもよい。変数生成機構96からの出力である8ビットは、データ・ベース12から得られた64ビットの暗号化されたPIN+PADのうちの56ビットと連結されそして段階98において通信キーCを用いてDESにより暗号化される。この結果としての64ビットは、データ・ベース12からの、暗号化されたPIN+PADの残りの8ビットと連結されて、取引応答メッセージのために、72ビットの2重に暗号化された欄を作り出す。

第9図を参照して、取引応答メッセージ42を受け取つた端末装置20によつて行なわれる処理

(26)

過程を示す。段階100において応答メッセージの基本部分中の選ばれた欄に対して基本的な認証検査が行なわれる。もしこの検査の結果、取引が承認されないと決まつたときには段階102において取引は終了し、段階104において取引状況メッセージがホスト10へ送られる。

もし取引が無条件に承認されれば、端末装置20が、段階106において取引を完了し、状況メッセージを送り返す。

もし取引が条件付きで承認されたときには、利用者は新しいPINを1度ないし数度入力でき、そのPINとデータ・ベースに記憶されていた暗号化されているPIN+KEYとの対応性が端末装置20において検査されることになる。場合によってはさらに用心のために変数の検査が付け加えられることもある。

段階108においては、第10図に示された手順に従つて暗号化された認証データ90が復号される。段階110においては変数生成機構によりホスト側で生成された変数欄が、端末装置20に

(27)

に従つて暗号化することもでき、認証データ90は第10図、段階116の手順により1回復号される。

第10図を参照する。ここでは端末装置20において行なわれる処理過程を記述する。

ここでは段階114(第9図)において、新たに入力されたPINと、データ・ベース12に記憶するために暗号化されたPINを比較する検査の準備として、すでに暗号化されている認証欄90を2重に復号する。まず、段階116においては通信キーCが用いられDESによつて認証欄90の72ビット中の64ビットが復号される。結果としての64ビットのうち56ビットは認証欄90の残りの8ビットと共に、1重に復号された(すなわち1重に暗号化された)PIN+PAD118を形成する。復号の段階116の結果としての64ビット中、残りの8ビットはホスト10において、変数生成機構により生成された変数であり、第9図の段階110における検査に用いられる。1重に暗号化されたPIN+PADはホス

(29)

特開昭56-123066(8)

よつて事前に(または再び)生成された変数と比較検査される。この検査は、もし変数生成機構が乱数を生成する場合には行なわれない。もしこの付加的な変数検査が合格しなかつた場合には、取引は中止される。

段階112において利用者はPINを鍵盤32から入力するよう指示される。この、新たに入力されたPINは最初に入力されたもの(第4図におけるPIN54)とは異なるものになるであろう。これは利用者が正しいPINを忘れて、もういちど打鍵するような場合に行なわれる。段階114において新たに入力されたPINは、ホスト・データ・ベースからのPINと比較され、その結果が等しければ取引承認状況となり、段階106における取引が可能となる。もし等しくなければ、何回か決められた回数だけ入力が繰返され取引が終了する。段階114の比較の準備において暗号化されたデータ90は、第10図に示された手順に従つて2重に復号される。あるいは新たに入力されたPINは、第4図、段階56の手順

(28)

トのデータ・ベース12に記憶されているものと同一番号である。段階120において、こんどはPINキー50を用いてこれは再度DESにより復号され、新たに入力されたPINと比較できるよう完全に復号されたPIN番号を作り出す。

本発明を実施する最善の方法

第1図および第2図に関連し、以下、この発明による取引実行システムの動作を説明する。端末装置20において、取引要求メッセージ40が生成される。このメッセージ中には鍵盤32から入力された個人暗証番号が含まれており、この番号は二つのキーにより2重に暗号化される。またこのメッセージ中にはカード読取装置30によつて読み取られた、データ・ベースにアクセスするためのデータも含まれている。要求メッセージ40はホストCPU10へ送られる。

ホストCPU10においては、要求メッセージ40からデータ・ベース12にアクセスするための番号が抜き出され、データ・ベース12から認証番号(これは1重に暗号化されたPINである)

(30)

を取り出すのに用いられる。要求メッセージ40からの2重に暗号化された個人認証番号は、通信キーを用いて復号され、データ・ベースから取り出された、1重に暗号化されたPINと比較される。両者が等しくなれば、データ・ベース12からの、1重に暗号化されたPINは通信キーによつて更に暗号化される。この、結果的に2重に暗号化されたPINは取引応答メッセージに乘せられて端末装置20へ送り返され、取引の条件付き承認であることを示す。

端末装置20は、利用者に鍵盤32から改めてPINを入力するよう指示する。取引応答メッセージ42からの、2重に暗号化されたPINは2重に復号され、新たに入力されたPINとの一致性が検査される。そしてもしPINが一致すれば取引は完了する。

業界への適用の可能性

既述した取引実行システムをこの発明にしたがつて操作すれば、カード・データからの暗号化に

(31)

第8図は取引が拒否された時又は暗号化された比較データが等しい時の取引応答メッセージのフォーマットを示す図、第9図は端末装置における取引応答メッセージに回答したホストへの状況メッセージの発生を示す動作流れ図、第10図は端末装置における取引応答メッセージで受信された暗号化されたデータからの正当性データの発生を示す動作ブロック図、第11図は取引が条件付きで承認されたが承認を完了するためには端末装置におけるPIN検査を必要とする時の取引応答メッセージのフォーマット図である。

10・・・B銀行CPU、12・・・データ・ベース、16・・・A銀行CPU、18・・・データ・ベース、20・・・端末装置、30・・・カード読取装置、32・・・鍵盤、46・・・金融機関テーブル、60・・・変数生成機構。

出 願 人 インターナショナル・ビジネス・マシーンズ・コーポレーション

代 理 人 弁 理 士 頼 官 孝 一
(外1名)

(35)

よらず、しかもホストへそのつど通信せずに、利用者から数回にわたる入力によつてPINの認証が可能になる。これは特に提携銀行間において、PINが複数の銀行を通して通信されるさいに、安全な暗号化された形で行なわれるところに価値がある。

4. 図面の簡単な説明

第1図は代表的な取引実行システムを表わすブロック図、第2図は第2の代表的な取引実行システムにおける基本的な通信メッセージを示す図、第3図は第1図の取引実行システムにおける基本的な通信メッセージを示す図、第4図は端末装置における取引要求メッセージの発生を示す動作ブロック図、第5図はホストにおける条件付き取引承認メッセージの発生を示す動作流れ図、第6図はホストにおける取引要求メッセージからの暗号化されたPIN+PADの発生を示す動作ブロック図、第7図はホストにおける条件付き取引承認メッセージのためのデータ・ベースからの暗号化された認証データの発生を示す動作ブロック図、

(32)

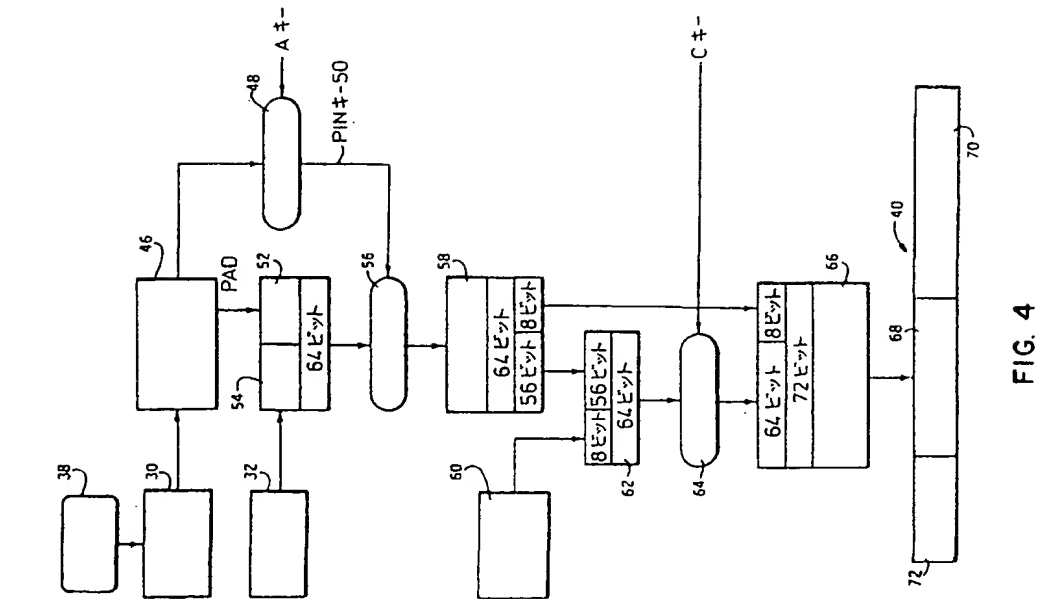


FIG. 4

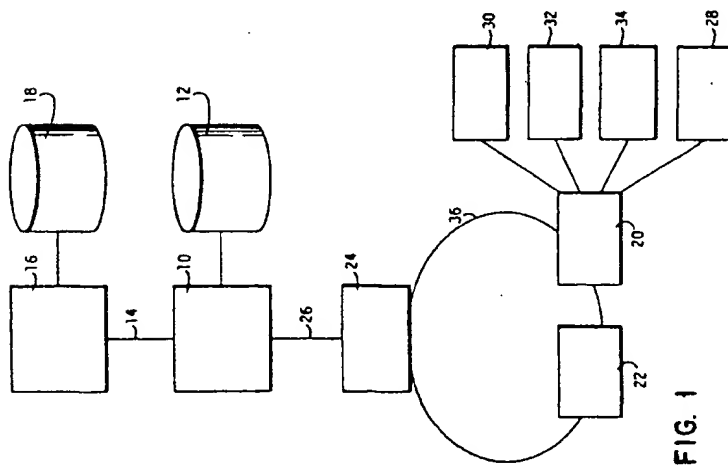


FIG. 1

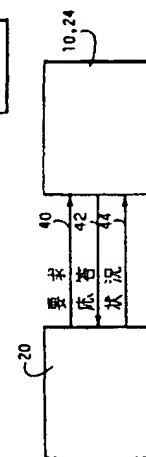


FIG. 2

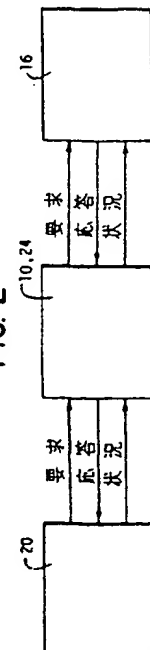


FIG. 3

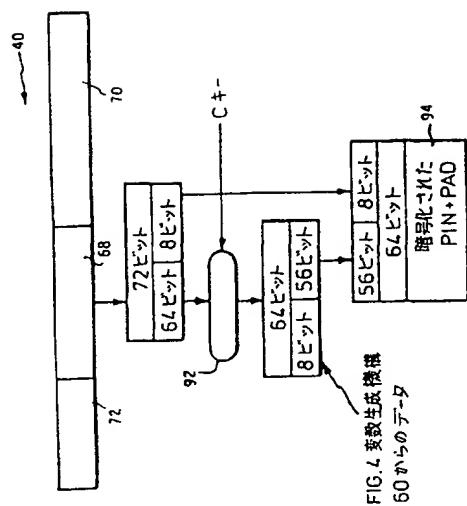


FIG. 6

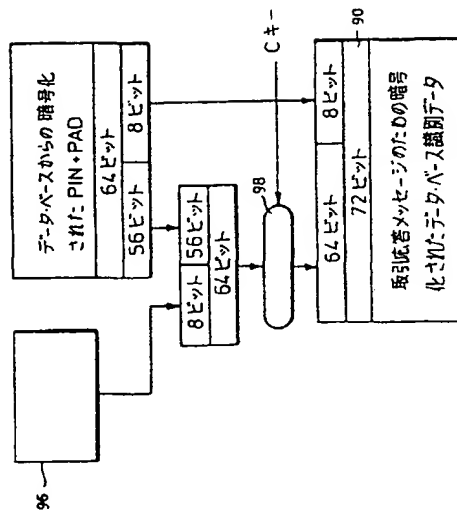
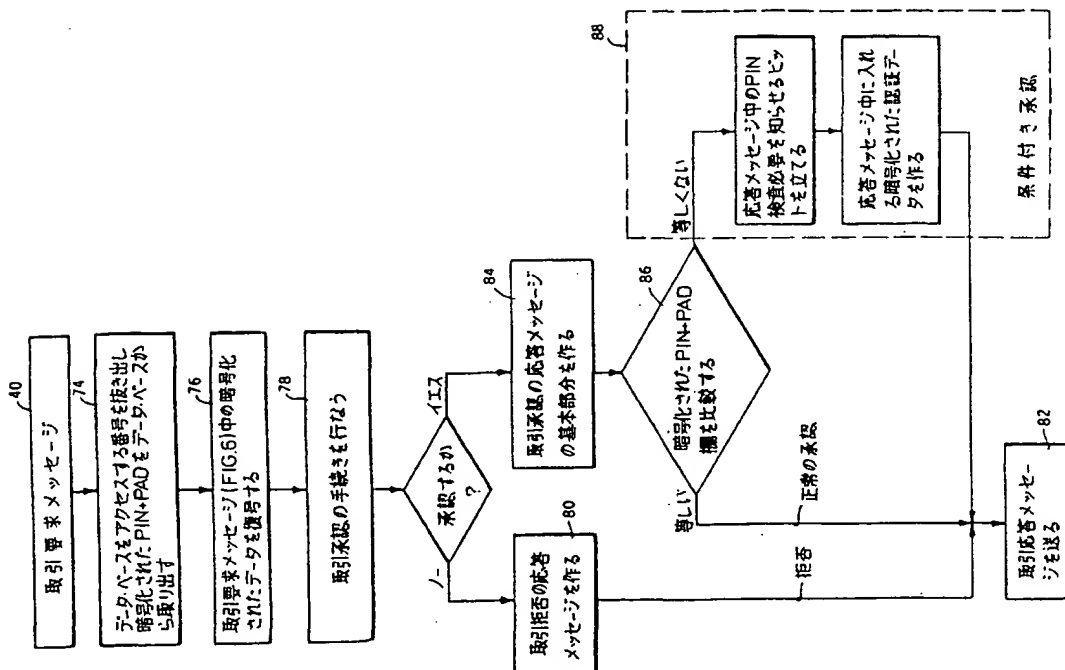


FIG. 7



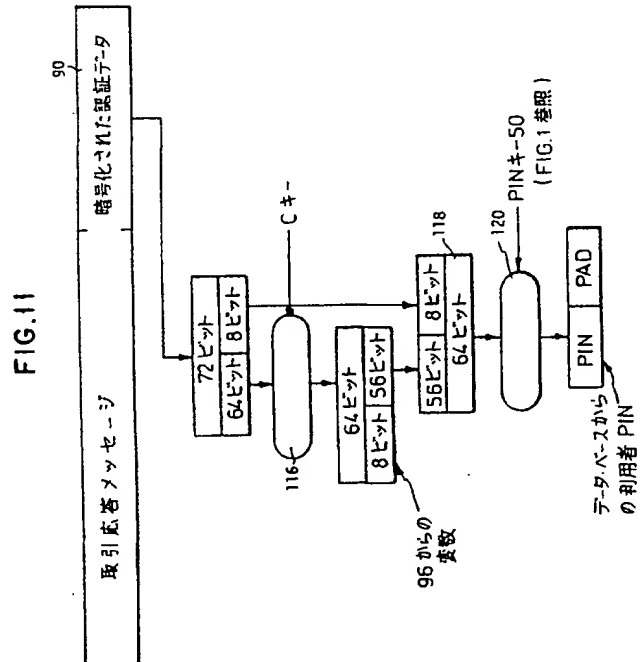
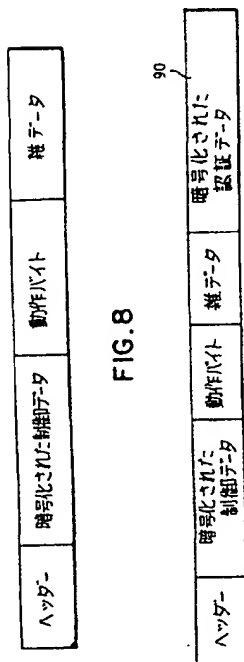
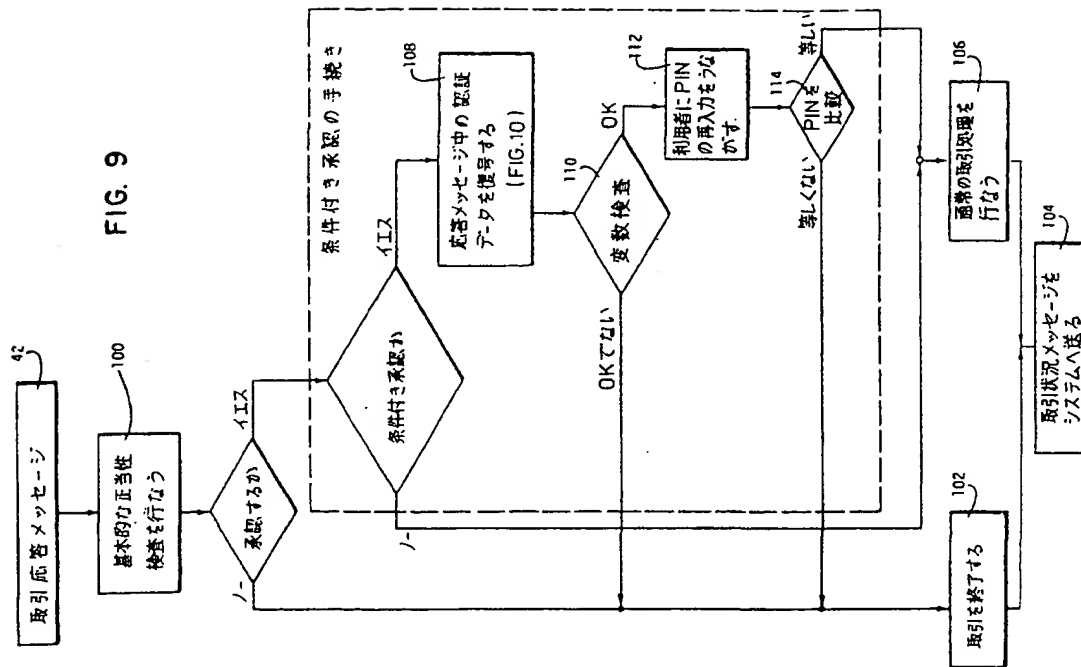


FIG. 10

**This Page is Inserted by IFW Indexing and Scanning
Operations and is not part of the Official Record**

BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images include but are not limited to the items checked:

- ☐ **BLACK BORDERS**
- ☐ **IMAGE CUT OFF AT TOP, BOTTOM OR SIDES**
- ☐ **FADED TEXT OR DRAWING**
- ☐ **BLURRED OR ILLEGIBLE TEXT OR DRAWING**
- ☐ **SKEWED/SLANTED IMAGES**
- ☐ **COLOR OR BLACK AND WHITE PHOTOGRAPHS**
- ☐ **GRAY SCALE DOCUMENTS**
- ☐ **LINES OR MARKS ON ORIGINAL DOCUMENT**
- ☒ **REFERENCE(S) OR EXHIBIT(S) SUBMITTED ARE POOR QUALITY**
- ☐ **OTHER:** _____

IMAGES ARE BEST AVAILABLE COPY.

As rescanning these documents will not correct the image problems checked, please do not report these problems to the IFW Image Problem Mailbox.